



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,507	03/26/2004	Ryogo Yanagisawa	2004-0472A	8594

513	7590	07/18/2007
WENDEROTH, LIND & PONACK, L.L.P.		
2033 K STREET N. W.		
SUITE 800		
WASHINGTON, DC 20006-1021		

EXAMINER
WANG, HARRIS C

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
07/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/809,507	YANAGISAWA, RYOGO	
	Examiner	Art Unit	
	Harris C. Wang	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☒ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>8/01/2006, 7/20/2004</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-19 are pending

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goss (4956863).

Regarding Claims 1-2, 5-6, 9-10, 13-14, 18-19

Goss teaches a key exchange apparatus including:

a random number generator for generating a random number k_a that holds a relationship $0 < k_a < q$, where q is an element in a finite group F for which multiplication is defined and an order that is a prime number of the element g is q ; (*"The first step in establishing the session key is that each user generates a secret number in a random number generator 14, 16. The numbers are designated X_a , X_b respectively, and are selected from a set of positive integers up to $p-1$ " Column 6, lines 23-27*)

Art Unit: 2139

a secret key holding unit for temporarily holding the random number k_a ; (*"Storage area 40 contains a preselected number X_a , stored at the time of manufacture of the A device"* Column 7, line 52)

a public key generator for calculating a public key y_a in the finite group F from the random number k_a , the element g , and the prime number q ;

($Y_a = a^{x_a} \bmod(p)$, $Y_b = a^{x_b} \bmod(p)$) (Column 6, lines 30-35)

and a shared key generator for calculating a shared key K_a in the finite group F using a public key y_b generated from a random number k_b which holds a relationship $0 < k_b < q$ and is generated by a second user as a destination distribution of the shared key, and the random number k_a that is held by the secret key holding unit, (*"Each user also has a session key generator 18, 20...After the exchange of values Y_a , Y_b , each user computes a session key K in its session key generator 18, 20 by raising the other user's Y value to the power represented by the user's own X value, all modulo p "* Column 6, lines 27-28, 55-60)

a controller of a first user as a distribution source of the shared key controlling the random number generator and the public key generator for obtaining the public key y_a , and transmitting the obtained public key y_a to a second user as a distribution destination of the shared key, and said controller obtaining the public key y_b from the second user as the shared key distribution destination, and controlling the shared key generator for deriving the shared key K_a . (*"The key management steps previously described proceed automatically under the control of the cryptographic processor 60, and when a session key has been derived, this is automatically applied in a conventional cryptographic process"* Column 12, lines 25-30)

Goss does not explicitly teach where at least said random number generator, said secret key holding unit, said public key generator, and the shared key generator being formed on one semiconductor integrated circuit.

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the method of Goss on one semiconductor integrated circuit.

The motivation is that the method of Goss has been known in the art for almost two decades, and one of ordinary skill in the art would be able to implement this method on one semiconductor integrated circuit.

The methods associated with the apparatus are taught in the cited sections.

Regarding Claim 3, 7, 11,15,

Goss teaches the key exchange apparatus of claim 13.

Goss does not explicitly teach wherein when the finite group F is an elliptic curve $E(F)$ in a finite field, and an element on the elliptic curve $E(F)$ is G , the public key generator calculates the public key y_a on the elliptic curve $E(F)$ using the random number k_a , the element G , and the prime number q by a formula: $y_a = k_a G \bmod q$, and the shared key generator calculates the shared key K_a on the elliptic curve $E(F)$ by a formula: $K_a = K_a y_b \bmod q$, using the public key $y_b = k_b G \bmod q$ that is generated from the random number k_b on the elliptic curve $E(F)$ by the second user as the shared key

Art Unit: 2139

distribution destination, and the random number k_a that is held in the secret key holding unit.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the finite group F as an elliptic curve $E(f)$ in a finite field, and an element on the elliptic curve $E(f)$ is G .

The motivation is that the Applicant in the background of the invention admits that "An elliptic curve crypto system is widely known as a cryptosystem based on the difficulty in solving the discrete logarithm problem in the finite group F . More specifically, when assuming an elliptic curve in the finite group as $E(F)$ a point on the elliptic curve $E(F)$ which is previously shared by the user 1 and the user 2 as G , and an arithmetic xG using a point x on the elliptic curve $E(f)$ is defined." Therefore one of ordinary skill in the art would be able to use the apparatus of Goss to implement a system using an elliptic curve in a finite field

Regarding Claims 4, 8, 12, 16-17,

Goss teaches the key exchange apparatus of claim 13 wherein the random number generator generates a new random number k_a after each new exchange of message traffic. (*"Ideally, a new session key should be established for each exchange of message traffic. An additional unsecured exchange is needed to accomplish this. The number generator in the A device generates a random number...and the number generator in the B device generates a random number...these are supplied to the session key generators 18, 20 respectively"* column 8, lines 46-54)

Art Unit: 2139

However Goss does not explicitly teach generating said random number after the calculation of the shared key K_a or the calculation of the public key Y_a , nor does Goss explicitly teach holding the new random number k_a in the secret key holding unit.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Goss to either regenerate a new random number after the calculation of the shared key K_a or the calculation of the public key Y_a , and subsequently store the random number in the storage unit.

The motivation is that it is clear that for each session there requires a new session key which requires a new random number to be generated. Whether the new random number is generated after the shared key K_a or the public key Y_a is an obvious modification, to the cited art in Goss which discloses that the new random number must be generated before the start of the next session.

Conclusion


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harris C. Wang whose telephone number is 5712701462. The examiner can normally be reached on M-F 8-5:30, Alternate Fridays Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ R. SHEIKH can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2139

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100